REMARKS

The claims remaining in the present application are Claims 1-19. The Examiner is thanked for performing a thorough search.

DRAWINGS

In paragraph 2, the Office Action requested a replacement for Figure 2. A formalized version of Figure 2 is included herewith. Therefore, Applicants believe that this objection has been addressed.

CLAIM REJECTIONS

35 U.S.C. §102

Claims 1-7 and 14-19

In paragraph 4, the Office Action rejected Claims 1-7 and 14-19 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication No. 20030188189 by Desai et al. (referred to hereinafter as "Desai"). Applicants respectfully submit that embodiments of the present invention are neither taught nor suggested by Desai.

Claim 1 recites,

> A method for configuring templates, the method comprising:
> configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template;
> configuring the template with second information for processing the data associated with at least one of the received messages; and
> configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system. (emphasis added)

Applicants respectfully submit that Desai does not teach or suggest any of the features recited by Claim 1.

Desai teaches a multi-level and multi-platform intrusion detection and response system that collects and analyzes log events (also referred to by Desai as data sets). For example in Paragraph 0043, Desai states, "As the log events are

created...log events are sent...to a secure central log/event collector 20, where they are collected for further processing. The log events are securely stored at the central log/event collector 20 in an associated event database 25, for example." In paragraph 0049, Desai states, "After the data collect is accomplished (step 81), the log events are processed thru an Event Analysis Engine 30..." At paragraph 0050, Desai states, "...each event is first parsed in step 51 so that data elements are identified and tagged..." At paragraph 0051, Desai states, "...the events are normalized ... (e.g., fields re-ordered and adjusted for size, data type, format, etc.), and assigned a Category based upon origination (e.g., Industry, Alert Source, etc.)." In paragraph 0052, Desai states, "After the normalization process, a search for a match may be conducted against a Known Offender or attack signature database." In paragraph 0053, Desai states, "...the events are de-duplicated and compared against established thresholds to weed out probably false positives. More specifically, after the data is collected, parsed, normalized and categorized, the present invention then applies sophisticated filtering techniques ... to substantially streamline problem diagnosis" (emphasis added). Paragraph 0054 states, "...the filters statistically qualify the data, and then compare the findings within the normal performance envelope..."

The Office Action asserts that Desai teaches "configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template," as recited by Claim 1 at lines 1-5 of paragraph 0022, lines 1-5 of paragraph 0023, lines 3-6 of paragraph 0093 and lines 6-8 of paragraph 0094.

Lines 1-5 of paragraph 0022 state, "A fourth object of the present invention is to provide an Intrusion Detection and Response system which identifies log-based abnormal behavior by employing pre-defined templates based upon on the type-profile of an enterprise." Note that Lines 1-5 of paragraph 002 say nothing about "...determining whether data associated with at least one message received by the template should or should not be processed by the template," (emphasis added).

Lines 1-5 of paragraph 0023 state, "A fifth object of the present invention is to provide an Intrusion Detection and Response system which identifies knowledge-based attack signatures by employing pre-defined templates based upon the type-profile of an enterprise." Again note that lines 1-5 of paragraph 0023 say nothing about "...determining whether data associated with at least one message received by the template should or should not be processed by the template," (emphasis added).

Paragraph 0093 states,

> Network-based system sensors can be configured to automatically respond to intrusion attempts before they have a chance to do any damage. Responses might include: (i) kill or reset malicious TCP connections; (ii) block offending IP address's on firewalls; or (iii) execute any user-defined programs or batch files.

Lines 6-8 of Paragraph 0094 state,

> The sensor must learn what is, and is not, acceptable traffic on any given segment. This period of adjustment is often referred to as the tuning or foot print period.

Note that paragraphs 0022 and 0023 refer to pre-defined filters that are applied after data is collected, parsed, normalized, and categorized. In citing paragraphs 0093 and 0094, the Office Action is now asserting that Network-based system sensors teach Claim 1's filters. First, network-based system sensors are not filters. Second, Desai's filters cannot be relied on to teach certain features of Claim 1's filters and then Desai's sensors relied on to teach other features of Claim 1's filters. Third, for reasons provided herein, neither Desai's sensors nor Desai's filters provide features as recited by Claim 1.

The Office Action asserts that Desai teaches "configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system" at lines 1-4 of paragraph 0063. Lines 1-4 of paragraph 63 state,

> After the Data Threshold Comparison and Analysis step 83 is performed, the events are then assigned a severity (step 57 of FIG. 5) and presented to the centralized management center for further analysis and response.

Note that lines 1-4 of paragraph 0063 say nothing about either Desai's sensor or Desai's filters let alone teach or suggest configuring a template to prevent communication of a received message to another template. Further, Desai's templates are not used in this manner. Instead as described in paragraphs 0053 and 0054, Desai's templates are applied to data after the data has been collected, parsed, normalized and categorized to streamline problem diagnosis. For example, Desai states at paragraph 0054, "...the filters statistically qualify the data, and then compare the findings within the normal performance envelope..."

For at least these reasons, independent Claim 1 should be patentable. For similar reasons independent Claims 8 and 14 should also be patentable. Claims 2-7 depend on Claim 1. Claims 9-13 depend on Claim 8. Claims 15-19 depend on Claim 14. These dependent claims include all of the features of their respective independent claims. Further, these dependent claims include additional features which further make them patentable. Therefore, these dependent claims should be patentable for at least the reasons that their respective independent claims should be patentable.

35 U.S.C. §102

Claims 8-13

Claims 8-13 are rejected under 35 U.S.C. §103(a) as being anticipated by Desai in view of U.S. Patent No. 6,957,348 by Flowers et al. (referred to hereinafter as "Flowers"). Applicants respectfully submit that embodiments of the present invention are neither taught nor suggested by Desai or Flowers, alone or in combination.

Independent Claims 1 and 14 are patentable over Desai. For similar reasons, Claim 8 should be patentable over Desai. Flowers does not remedy the deficiency in Desai. In fact the only part of Claim 8 that the Office Action asserts

that Flowers teaches is a guideline. Therefore Claim 8 should be patentable. Claims 9-13 depend on Claim 8 and include all of the features of Claim 8. Therefore Claims 9-13 should be patentable for at least the reasons that Claim 8 should be patentable.

CONCLUSION

In light of the above listed amendments and remarks, reconsideration of the rejected claims is requested. Based on the arguments and amendments presented above, it is respectfully submitted that Claims 1-19 overcome the rejections of record. For reasons discussed herein, Applicants respectfully request that Claims 1-19 be considered be the Examiner. Therefore, allowance of Claims 1-19 is respectfully solicited.

Should the Examiner have a question regarding the instant amendment and response, the Applicant invites the Examiner to contact the Applicants' undersigned representative at the below listed telephone number.

Respectfully submitted,
WAGNER BLEHCER LLP

Dated: 8/15/, 2007

John P. Wagner Jr.
Registration No. 35,398

Address: Westridge Business Park
123 Westridge Drive
Watsonville, California 95076 USA

Telephone: (408) 377-0500 Voice
(408) 234-3649 Direct/Cell
(831) 722-2350 Facsimile